Remarks

Claims 1 and 9 have been amended for clarification purposes and to correct typographical and administrative errors. Applicants reserve the right to pursue the original claims and other claims in this application and in other applications. Claims 1 and 9-18 are pending in this application.

Claims 9-18 stand rejected under 35 U.S.C. § 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, the Office Action contends the specification , as originally filed, does not provide support for a "token key used to generate a digital token" (claim 9, line 13), "the second cryptographic key further including a third key" (claim 9, lines 13-14), "using the token key to generate a digital token" (claim 14, lines 11-12) and "the first, second, third and fourth keys are identical" (claim 11). Applicants respectfully disagree.

With respect to a token key used to generate a digital token, the Examiner's attention is directed to the Specification, page 10, line 31 to page 11, line 11, which states:

> "Data Center 30 also includes a meter box 44 that shares a secret key with the steel box for decrypting the token key encrypted in the meter record. Meter box 44 also holds the key used for digital signature of transaction records, which are stored in Database Server 36. The only other information stored in meter box 44 is freshness data for each meter record processed by meter box 44. For each postage transaction, meter box 44 generates at least one digital token or signs the postage transaction, and updates the meter record corresponding to the transaction. Each meter record in Database Server 36 includes postal funds as well as the token keys in cipher text. Meter box 44 uses the token keys to generate tokens, updates the postal funds in the meter record, and signs the updated meter record. In this manner, meter box 44 performs and controls the secure accounting for each transaction. Meter box 44 can also be used to verify the token or the transaction signature for verification of the postage evidencing for the transaction." (Emphasis added).

Claim 9, lines 13-14 have been amended to recite the "second cryptographic module further including a third key." The Examiner's attention is directed to the Specification, pages 15-16, and Fig. 5, which describe the process performed within the secure meter box 44. Specifically, the meter box 44 decrypts the token key that was received in encrypted form as part of the meter record (step 235) using a key (second key). The meter box 44 then signs the updated meter record (transaction record) using a key (third key) stored in the meter box 44 (step 260).

With respect to the first, second, third and fourth keys being identical, the Examiner's attention is directed to the Specification, page 13, lines 8-11, which states:

> "In the preferred embodiment of the present invention, one common key is used to sign all transactions and records that require a digital signature, such a, meter records, postage transactions, funds transfer records, master account records, etc." (Emphasis added).

A common key means the keys have the same value, i.e., they are identical.

Claims 9-13 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Reconsideration is respectfully requested.

Claim 9 has been amended to provide the proper antecedent basis for "remote processor" in line 3.

With respect to claim 11, the Office Action contends it cannot be clearly understood what "identical" means. Identical means the same. A key for cryptography, as is well known, can be any one of a large number of values. Thus, if keys are identical, it means they have the same value. Applicants respectfully submit that the term "identical" is not indefinite.

Claim 1 stands rejected under 35 U.S.C. §102(e) as being anticipated by Kara (U.S. Patent No. 5,822,739). Claim 1 has been amended to clarify that the database is

located at the data center. Reconsideration of claim 1 as amended is respectfully requested.

The present invention is directed to a virtual postage metering system and method. Claim I as amended recites a method for evidencing postage that comprises "generating a digital token . . . including encrypted information for the mailpiece . . . creating a transaction record . . . including the digital token and the postal information; signing the transaction record" and "storing the transaction record in a database at the data center."

The Office Action contends that Kara discloses signing the transaction record and storing the transaction record in a database at Col. 14, lines 12-36. Applicants respectfully disagree. In the present invention, a key is used to sign the transaction record, thus creating a digital signature. The signed transaction record is stored in a database at the data center. The Office Action contends that a transaction record having a "unique transaction identifier" is equivalent to signing a transaction. The unique transaction identifier in Kara is merely an identifier of the transaction, such as, for example, a serial number or the like. Thus, the information contained within the transaction record can be altered or changed. The "unique transaction identifier" does not provide any type of protection against such alteration, nor does it provide any type of authentication of the author. A digital signature, in contrast, authenticates and protects the integrity of the information in the transaction record. Thus, the signed record is unalterable and the signature cannot be repudiated. These attributes are not inherently present in a "unique transaction identifier" as contended by the Office Action. The Examiner is respectfully requested to provide a basis in fact and/or technical reasoning to reasonably support the determination that a "unique transaction identifier" would inherently have the same characteristics as a digital signature as described above. (See *Ex parte Levy*, 17 USPQ2d, 1461, 1464 (Bd. Pat. App. & Inter. 1990)).

Furthermore, in Kara, a meter program is used to generate a data packet that is a digital representation or image of the postage indicia to be ultimately printed by the demanding site. The data packet includes information required of a valid postage indicia by a postal service. (Col. 14, lines 30-41). Thus, the data packet is sent to the demanding

site for use in printing the indicia. Specifically, at step 308 of Fig. 3, the data packet generated from the received demand is transmitted via the data communications link to the demand site. (Col. 15, lines 1-3). There is no disclosure, teaching or suggestion in Kara of creating a transaction record, signing the transaction record, and storing the signed transaction record in a database at the data center as is recited in claim 1.

For at least the above reasons, Applicants respectfully submit that claim 1 is allowable over the prior art of record.

Claims 9-18 stand rejected under 35 U.S.C. §102(e) as being anticipated by, or, in the alternative, under 35 U.S.C. § 103(a) as obvious over, Whitehouse (U.S. Patent No. 6,005,945). Reconsideration is respectfully requested.

Claim 9 is directed to a system for dispensing postage that includes a data center, the data center comprising a "storage device," a "first cryptographic module" that includes a "first key to decrypt a user authentication key included in the user account, the user authentication key being used to authenticate the user; and a second cryptographic module . . . including a second key to decrypt a token key included the meter account, the token key used to generate a digital token, the second cryptographic module further including a third key used to sign a transaction record associated with generating the digital token, the signed transaction record being stored in the storage device."

Whitehouse is directed to a system for the electronic distribution of postage wherein all secure processing required for generating postal indicia is performed at secure central computers, not at end user computers, thereby removing the need for specialized secure computational equipment at end user sites. In Whitehouse, a typical secure central computer includes a data processor and a database of information concerning user accounts of users authorized to request postal indicia from the secure central computer. A request validation procedure authenticates received postage request with respect to the user account information in the database. A postal indicia creation procedure applies a secret encryption key to information in each authenticated postage request so as to generate a digital signature and combines the information in each authenticated postage

request with the corresponding generated digital signature so as to generate a digital postage indicium in accordance with a predefined postage indicium data format. A communication procedure securely transmits the generated digital postage indicium to the requesting end user computer. (Col. 6, lines 20-45).

In Whitehouse, the data stored by the secure central computer 102 in its customer database for each meter/user account includes various information related to the account. In addition, for each meter or account, at least two child transaction tables are maintained in the transaction database 174. The first is a record of postage purchases, and the second transaction table records each postage indicium dispensing event. Whitehouse further indicates that storing data on the central computer offers very distinct advantages over conventional meters or the PSD, since the meter balances are stored on computer media rather than secure non-volatile meter registers. (Col. 10, line 45 to Col. 11, line 56).

Thus, although Whitehouse may store significant amounts of data at the central computer, there is no disclosure, teaching or suggestion in Whitehouse of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9. In fact, Applicants respectfully submit that Whitehouse teaches away from the present invention, since as noted above Whitehouse indicates that storing data on the central computer offers very distinct advantages over conventional meters or the PSD, since the meter balances are stored on computer media rather than secure non-volatile meter registers. Thus, the data stored in Whitehouse is not secured as is done in the present invention by signing the transaction records before storing them. Thus, there is no disclosure, teaching or suggestion in Whitehouse of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

Although Whitehouse discusses the use of a digital signature, this signature is added to the other parts of the postage indicium and a message, including data representing the postage indicium with the digital signature, is encrypted and then the resulting message is transmitted to the requesting user. (Col. 13, line 15-50). This is not

the same as signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

For at least the above reasons, Applicants respectfully submit that claim 9 is allowable over the prior art of record. Claims 10-13, dependent upon claim 9, are allowable along with claim 9 and on their own merits.

Claim 14 includes limitations substantially similar to those of claim 9. For the same reasons given with respect to claim 9 above, Applicants respectfully submit that claim 14 is allowable over the prior art of record. Claims 15-18, dependent upon claim 14, are allowable along with claim 14 and on their own merits.

In view of the foregoing amendments and remarks, it is respectfully submitted that all claims of this case are in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,

Brian A. Lemm
Reg. No. 43,748
Attorney for Applicants
Telephone No.: (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

MARKED VERSION TO SHOW CHANGES

In the Claims:

Amend claims 1 and 9 as follows:

1. (Amended) A method for evidencing postage on a mailpiece comprising the steps of:

receiving at a data center postal information relating to a mailpiece, said postal information including recipient address information for the mailpiece;

generating a digital token for the mailpiece, said digital token including encrypted information for the mailpiece based on said recipient address information;

creating a transaction record, said transaction record including the digital token and the postal information;

signing the transaction record;

storing the transaction record in a database at the data center; and

performing value added services using the transaction record.

9. (Amended) A system for dispensing postage value comprising:

a data center communicatively coupled to a remote processor [computer] via a network, a user initiating a request to the data center via the remote processor to dispense postage value to be printed by a printer coupled to the remote processor, the data center comprising:

a storage device to store data records, the data records including a user account and a meter account associated with the user;

a first cryptographic module coupled to the storage device, the first cryptographic module including a first key to decrypt a user authentication key included in the user account, the user authentication key being used to authenticate the user; and

a second cryptographic module coupled to the storage device, the second cryptographic module including a second key to decrypt a token key included in the meter account, the token key used to generate a digital token, the second cryptographic module [key] further including a third key used to sign a transaction record associated with generating the digital token, the signed transaction record being stored in the storage device;

wherein the data center sends the digital token to the remote processor via the network.